SYSTEM AND METHOD FOR ENCRYPTING BROADCAST PROGRAM

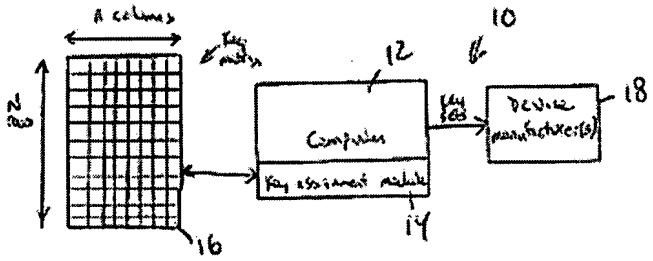
Publication number: JP2000031922
Publication date: 2000-01-28
Inventor: JEFFREY BRUCE LOTSPEACH; KEVIN SNOW MACURLEY
Applicant: IBM
Classification:
- International: ***H04H1/00; H04L9/00; H04L9/08; H04N7/167;*** **H04H1/00; H04L9/00; H04L9/08; H04N7/167;** (IPC1-7): H04H1/00; H04L9/08; H04N7/167
- European: H04L9/00; H04L9/08; H04N7/167D
Application number: JP19990107957 19990415
Priority number(s): US19980065938 19980424

Also published as:
US6888944 (B2)
US6883097 (B1)
US6832319 (B1)
US6650753 (B1)
US6609116 (B1)
more >>

Report a data error here

Abstract of **JP2000031922**

PROBLEM TO BE SOLVED: To provide a transmission method of a digital program with security to in-home digital devices even when parts of the devices are not allowed by a digital broadcast system. SOLUTION: The system is provided with a matrix whose elements are device keys Si,j, where 'i' denotes a key index variable indicating a position in the matrix in terms of a key-dimension and 'j' shows a set index variable depicting a position in the matrix in terms of a set-dimension. This matrix is used to assign plural device keys each assigned to only one in-home device depending on each key index variable 'i'. In order to generate a session key for a broadcast program, all the device keys Si,j, are used to encrypt session numbers xi and to generate a session key block that is used to generate the session key that decodes the program by each in-home device. In the case that any of the devices is a device not permitted by the digital broadcast system a dummy number is assigned to at least a session number 50 that the dummy number is encrypted by a corresponding key for the device not permitted by the system and the resulting decoded session key is not useful to decode the program key.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－31922
（P2000－31922A）
(43)公開日　平成12年１月28日(2000.1.28)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｈ　1/00		Ｈ０４Ｈ　1/00	Ｆ	
Ｈ０４Ｌ　9/08		Ｈ０４Ｌ　9/00	６０１Ｅ	
Ｈ０４Ｎ　7/167			６０１Ａ	
		Ｈ０４Ｎ　7/167	Ｚ	

審査請求　有　請求項の数36　ＯＬ　（全 23 頁）

(21)出願番号　特願平11－107957

(22)出願日　平成11年４月15日(1999.4.15)

(31)優先権主張番号　０９／０６５９３８

(32)優先日　平成10年４月24日(1998.4.24)

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国10504、ニューヨーク州　アーモンク　（番地なし）

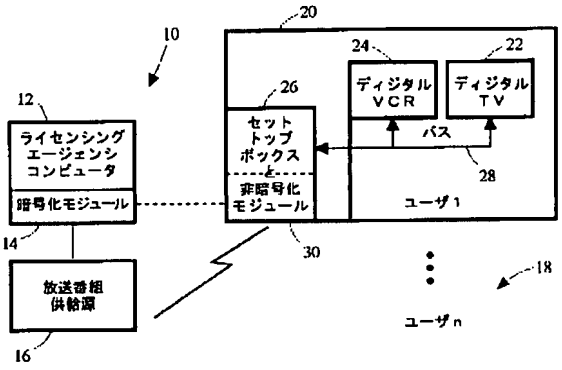
(72)発明者　ジェフリー・ブルース・ロッツピーチ
アメリカ合衆国95123　カリフォルニア州　サンノゼ　フットヒル・ドライブ　992

(74)代理人　100086243
弁理士　坂口　博　（外１名）

最終頁に続く

(54)【発明の名称】　放送番組を暗号化するためのシステムおよび方法

(57)【要約】
【課題】　ディジタル放送システムが、装置の一部が許可されないものである時でも家庭内ディジタル装置へのディジタル番組の保護された送信を提供する。
【解決手段】　装置鍵Ｓj,iの行列を設ける。ここで、「ｉ」は、行列の鍵次元での位置を示す鍵インデックス変数であり、「ｊ」は、行列の集合次元での位置を示す集合インデックス変数である。家庭内装置のそれぞれには、鍵インデックス変数「ｉ」ごとに１つの装置鍵だけが装置に割り当てられる形で、この行列からの複数の装置鍵が割り当てられる。放送番組用のセッション鍵を生成するために、すべての装置鍵Ｓj,iを用いてセッション番号xiを暗号化して、家庭内装置によって非暗号化され、番組を非暗号化するためのセッション鍵の生成に使用されるセッション鍵ブロックを生成する。装置のうちの１つが暗号漏洩された装置である場合には、少なくとも１つのセッション番号を、対応する暗号漏洩された装置鍵によって暗号化され、非暗号化され、結果のセッション鍵が番組の非暗号化に有用でなくなるダミー番号にする。



1

【特許請求の範囲】

【請求項１】装置鍵の集合から選択された複数のコンピュータ使用可能装置鍵をそれぞれが含む複数のユーザ装置と、

セッション鍵ブロックを作るために装置鍵の前記集合を用いて複数のセッション番号を暗号化するための少なくとも１つのセッション鍵ブロック・ジェネレータであって、前記装置のうちの少なくとも１つが暗号漏洩された装置鍵を定義する暗号漏洩された装置であると判定された時に前記セッション番号のうちの少なくとも１つがダミー番号になり、前記ダミー番号が少なくとも１つの暗号漏洩された装置鍵によって暗号化され、前記セッション鍵ブロックが番組の非暗号化に使用するために送信される、前記少なくとも１つのセッション鍵ブロック・ジェネレータと、

各ユーザ装置にアクセスでき、前記セッション鍵ブロックおよび前記装置のそれぞれの前記装置鍵に基づいてセッション鍵を判定するために前記装置の前記装置鍵にアクセスする非暗号化モジュールであって、前記セッション鍵が、前記装置が前記セッション鍵の生成に前記ダミー番号を使用しない限り、前記番組を非暗号化するためにユーザ装置によって使用可能である、前記非暗号化モジュールとを含む、１つまたは複数の放送番組を暗号化するためのシステム。

【請求項２】装置鍵の前記集合が、鍵次元および集合次元を含む少なくとも２次元の行列によって表され、前記鍵次元が、鍵インデックス変数「ｉ」によってそれぞれが表される「Ｎ」個の鍵位置を表し、前記集合次元が、集合インデックス変数「ｊ」によってそれぞれが表される「Ｍ」個の集合を表し、各装置鍵を$S_{j,i}$によって表すことができる、請求項１のシステム。

【請求項３】ある装置の２つの装置鍵のいずれもが、互いに同一の鍵インデックス変数「ｉ」を有しない、請求項２のシステム。

【請求項４】各セッション番号をx_iによって表すことができるように、鍵インデックス変数「ｉ」ごとにそれぞれのセッション番号が設けられ、各セッション番号x_iが、前記セッション鍵ブロックを作るために第ｉ鍵次元の装置鍵によってのみ暗号化される、請求項３のシステム。

【請求項５】暗号漏洩された装置鍵を有しないすべての装置が、少なくとも第１セッション鍵を生成し、暗号漏洩された装置鍵を有するすべての装置が、少なくとも第２セッション鍵を生成し、第１セッション鍵だけが前記番組の非暗号化に有用になるように、各装置が、前記第ｉセッション番号を非暗号化するためにそれぞれの第ｉ装置鍵$S_{j,i}$を使用する、請求項４のシステム。

【請求項６】前記第１セッション鍵を生成する装置が、少なくとも第１プールを定義し、前記第２セッション鍵を生成する装置が、少なくとも第２プールを定義し、前

2

記システムがさらに、前記第１プール内のすべての装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に前記第１プール内の前記装置に、前記装置が新しい装置鍵を生成するために操作する更新データを送信するためのコンピュータ可読コード手段を含む、請求項５のシステム。

【請求項７】前記第２セッション鍵を生成する装置が、少なくとも第２プールを定義し、前記システムがさらに、前記第２プール内のすべての装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合に前記第２プール内の装置に新しいセッション鍵を生成させるためのコンピュータ可読コード手段を含む、請求項５のシステム。

【請求項８】暗号漏洩されない装置の第１集合が、第１プールを定義し、暗号漏洩されない装置の第２集合が、第３プールを定義し、前記第１プールおよび前記第３プールのそれぞれが、暗号漏洩された装置を含まず、前記システムがさらに、前記第１プール内の装置に、そのセッション鍵を前記第３プール内の装置の前記セッション鍵によって置換させるためのコンピュータ可読コード手段を含む、請求項５のシステム。

【請求項９】ディジタル番組を放送するためにこれを暗号化するためのコンピュータ使用可能コード手段を有するコンピュータ使用可能媒体を含むデータ記憶装置を具備するコンピュータにおいて、前記コンピュータ使用可能コード手段が、

ｉが１とＮを含む１からＮまでの整数であり、ｊが１とＭを含む１からＭまでの整数であり、「ｉ」が装置鍵$S_{j,i}$の行列の鍵次元での位置を示す鍵次元インデックス変数であり、「ｊ」が前記行列の集合次元での位置を示す集合インデックス変数であり、「Ｎ」が鍵のＭ個の集合のそれぞれの装置鍵の個数であるものとして、前記装置鍵$S_{j,i}$の行列にアクセスするためのコンピュータ可読コード手段と、

鍵インデックス変数「ｉ」ごとに各ディジタル・ビデオ装置に１つの装置鍵だけが割り当てられるように、複数の前記ディジタル・ビデオ装置に装置鍵の前記行列からそれぞれの複数の装置鍵を割り当てるためのコンピュータ可読コード手段と、

ｉが１とＮを含む１からＮまでの整数であるものとして、各セッション番号x_iがそれぞれの鍵インデックス変数「ｉ」に対応するように複数の前記セッション番号x_iを生成するためのコンピュータ可読コード手段と、

ｊが１とＭを含む１からＭまでの整数であるものとして、セッション鍵ブロックを生成するために、すべての装置鍵$S_{j,i}$を用いて各セッション番号x_iを暗号化するためのコンピュータ可読コード手段とを含む、コンピュータ。

【請求項１０】前記ディジタル・ビデオ装置のうちの１つまたは複数が暗号漏洩された装置であるかどうかを判

定するためのコンピュータ可読コード手段と、
前記暗号漏洩された装置の少なくとも１つの暗号漏洩された装置鍵によって暗号化されるダミー番号として、前記セッション番号のうちの少なくとも１つを作るためのコンピュータ可読コード手段とをさらに含む、請求項９のコンピュータ。
【請求項１１】第１ディジタル・ビデオ装置が、第１セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第１ディジタル・ビデオ装置が、少なくとも第１プールを定義し、第２ディジタル・ビデオ装置が、第２セッション鍵を生成するために前記セッション鍵のうちの少なくとも一部を非暗号化し、前記第２ディジタル・ビデオ装置が、少なくとも第２プールを定義し、前記コンピュータがさらに、
前記第１プール内のすべての装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に前記第１プール内の前記ディジタル・ビデオ装置に、前記ディジタル・ビデオ装置が新しい装置鍵を生成するために操作する更新データを送信するためのコンピュータ可読コード手段を含む、請求項１０のコンピュータ。
【請求項１２】第２ディジタル・ビデオ装置が、第２セッション鍵を生成するために前記セッション鍵ブロックの少なくとも一部を非暗号化し、前記第２ディジタル・ビデオ装置が、少なくとも第２プールを定義し、前記コンピュータがさらに、前記第２プール内のすべての装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合に前記第２プール内の装置に新しいセッション鍵を生成させるためのコンピュータ可読コード手段を含む、請求項１０のコンピュータ。
【請求項１３】暗号漏洩されない装置の第１集合が、第１プールを定義し、暗号漏洩されない装置の第２集合が、第３プールを定義し、前記第１プールおよび前記第３プールのそれぞれが、暗号漏洩された装置を含まず、前記コンピュータがさらに、
前記第１プール内の装置に、そのセッション鍵を前記第３プール内の前記装置の前記セッション鍵によって置換させるためのコンピュータ可読コード手段を含む、請求項１０のコンピュータ。
【請求項１４】前記ディジタル・ビデオ装置と組み合わされた、請求項９のコンピュータ。
【請求項１５】ｉが１とＮを含む１からＮまでの整数であり、ｊが１とＭを含む１からＭまでの整数であり、「Ｎ」が鍵のＭ個の集合のそれぞれの装置鍵の数であるものとして、それぞれが「ｊ」装置鍵$S_{j,i}$によって暗号化されるセッション番号x_iを含み、少なくとも次元「ｉ」および「ｊ」を有する行列によって表現できるセッション鍵ブロックを受信するためのコンピュータ可読コード手段と、
変数「ｉ」ごとに１つだけディジタル・ビデオ装置に割り当てられる複数の局所装置鍵にアクセスするためのコンピュータ可読コード手段と、
前記局所装置鍵を使用して前記セッション鍵ブロックからのセッション鍵を非暗号化するためのコンピュータ可読コード手段とを含む、少なくとも１つのディジタル番組を受信し、提示するために構成された前記ディジタル・ビデオ装置のための非暗号化モジュール。
【請求項１６】さらに、前記ディジタル・ビデオ装置が暗号漏洩された装置鍵を有しない場合に、前記ディジタル・ビデオ装置が第１セッション鍵を生成し、前記ディジタル・ビデオ装置が１つまたは複数の暗号漏洩された装置鍵を有する場合に、前記ディジタル・ビデオ装置が第２セッション鍵を生成し、前記第１セッション鍵だけが前記ディジタル・ビデオ番組の非暗号化に有用になるように、第ｉセッション番号を非暗号化するためにそれぞれの第ｉ局所装置鍵を使用するためのコンピュータ可読コード手段を含む、請求項１５のモジュール。
【請求項１７】さらに、更新データを受信するためのコンピュータ可読コード手段を含み、前記モジュールが、１つまたは複数の新しい局所装置鍵を生成するために前記更新データを操作するために１つまたは複数の前記局所装置鍵を使用する、請求項１６のモジュール。
【請求項１８】さらに、放送メッセージに応答して、前記セッション鍵を他の装置のセッション鍵によって置換するためのコンピュータ可読コード手段を含む、請求項１７のモジュール。
【請求項１９】装置鍵の集合から選択された複数のコンピュータ使用可能装置鍵を複数のユーザ装置に供給するステップと、
セッション鍵ブロックを作るために装置鍵の前記集合を用いて複数のセッション番号を暗号化する少なくとも１つのセッション鍵ブロック・ジェネレータを生成するステップと、
前記ユーザ装置のうちの少なくとも１つが、暗号漏洩された装置鍵を定義する暗号漏洩された装置であることが判定された時に、前記セッション番号のうちの少なくとも１つがダミー番号になるように定義するステップと、
暗号漏洩された装置鍵を用いて前記ダミー番号を暗号化するステップと、
１つまたは複数の放送番組の非暗号化に使用するために前記セッション鍵ブロックを送信するステップと、
前記ユーザ装置がセッション鍵の生成に前記ダミー番号を使用しない限り、前記番組を非暗号化するためにユーザ装置によって使用可能な前記セッション鍵を、前記セッション鍵ブロックおよび前記ユーザ装置のそれぞれの前記装置鍵に基づいて判定するために各ユーザ装置の前記装置鍵にアクセスするステップとを含む、前記１つまたは複数の放送番組の保護された送信のためのコンピュータ実施される方法。
【請求項２０】装置鍵の前記集合が、鍵次元および集合

次元を含む少なくとも２次元の行列によって表現可能であり、前記鍵次元が、鍵インデックス変数「ｉ」によってそれぞれが表される「Ｎ」個の鍵位置を表し、前記集合次元が、集合インデックス変数「ｊ」によってそれぞれが表される「Ｍ」個の集合を表し、各装置鍵を$S_{j,i}$によって表すことができるようになっている、請求項１９の方法。

【請求項２１】あるユーザ装置の２つの装置鍵のどれもが、互いに同一の鍵インデックス変数「ｉ」を有しない、請求項２０の方法。

【請求項２２】各セッション番号をx_iによって表すことができるように、鍵インデックス番号「ｉ」ごとにそれぞれのセッション番号を供給するステップと、

前記セッション鍵ブロックを作るために、第ｉ鍵次元の装置鍵だけを用いて各セッション番号x_iを暗号化するステップとを含む、請求項２１の方法。

【請求項２３】前記暗号漏洩された装置鍵を有しないすべてのユーザ装置が、少なくとも第１セッション鍵を生成し、前記暗号漏洩された装置鍵を有するすべてのユーザ装置が、少なくとも第２セッション鍵を生成し、前記第１セッション鍵だけが、前記番組の非暗号化に有用になるように、各ユーザ装置が、第ｉセッション番号を非暗号化するためにそれぞれの第ｉ装置鍵$S_{j,i}$を使用する、請求項２２の方法。

【請求項２４】前記第１セッション鍵を生成するユーザ装置が、少なくとも第１プールを定義し、前記第２セッション鍵を生成するユーザ装置が、少なくとも第２プールを定義し、前記方法がさらに、

前記第１プール内のすべてのユーザ装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に、

前記第１プール内の前記ユーザ装置に、新しい装置鍵を生成するために前記ユーザ装置が操作する更新データを送信するステップを含む、請求項２３の方法。

【請求項２５】前記第２セッション鍵を生成するユーザ装置が、少なくとも第２プールを定義し、前記方法がさらに、

前記第２プール内のすべてのユーザ装置が、暗号漏洩された装置であるかどうかを判定し、そうでない場合に、

前記第２プール内のユーザ装置に新しいセッション鍵を生成させるステップを含む、請求項２３の方法。

【請求項２６】暗号漏洩されていない装置の第１集合が、第１プールを定義し、暗号漏洩されていない装置の第２集合が、第３プールを定義し、前記第１プールおよび前記第３プールのそれぞれが、暗号漏洩された装置を含まず、前記方法がさらに、

前記第１プール内の装置に、前記第３プール内の前記装置の前記セッション鍵を用いてそれぞれのセッション鍵を置換させるステップを含む、請求項２３の方法。

【請求項２７】ディジタル処理装置によって読み取ることができるコンピュータ・プログラム記憶装置と、

ディジタル番組の放送のためにこれを暗号化するための方法ステップを実行するために前記ディジタル処理装置によって実行可能な命令を含む、前記プログラム記憶装置上のプログラム手段とを含み、前記方法ステップが、

ｉが１とＮを含む１からＮまでの整数であり、ｊが１とＭを含む１からＭまでの整数であり、「ｉ」が装置鍵$S_{j,i}$の行列の鍵次元での位置を示す鍵インデックス変数であり、「ｊ」が前記行列の集合次元での位置を示す集合インデックス変数であり、「Ｎ」が鍵のＭ個の集合のそれぞれの装置鍵の数であるものとして、前記装置鍵$S_{j,i}$の行列にアクセスするステップと、

鍵インデックス変数「ｉ」ごとに各ディジタル・ビデオ装置に１つの装置鍵だけが割り当てられる形で、複数の前記ディジタル・ビデオ装置に、前記装置鍵の行列から複数の装置鍵を割り当てるステップと、

ｉが１とＮを含む１からＮまでの整数であるものとして、それぞれが鍵インデックス変数「ｉ」に対応する複数のセッション番号x_iを生成するステップと、

ｊが１とＭを含む１からＭまでの整数であるものとして、セッション鍵ブロックを生成するために、すべての装置鍵$S_{j,i}$を用いて各セッション番号x_iを暗号化するステップとを含む、コンピュータ・プログラム装置。

【請求項２８】前記方法ステップがさらに、

前記ディジタル・ビデオ装置のうちの１つまたは複数が暗号漏洩された装置であるかどうかを判定するステップと、

前記暗号漏洩された装置の少なくとも１つの暗号漏洩された装置鍵によって暗号化されるダミー番号として、前記セッション番号のうちの少なくとも１つを作るステップとを含む、請求項２７のコンピュータ・プログラム装置。

【請求項２９】第１ディジタル・ビデオ装置が、第１セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第１ディジタル・ビデオ装置が、少なくとも第１プールを定義し、第２ディジタル・ビデオ装置が、第２セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第２ディジタル・ビデオ装置が、少なくとも第２プールを定義し、前記方法ステップがさらに、

前記第１プール内のすべてのディジタル・ビデオ装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に、新しい装置鍵を生成するために前記第１プール内の前記ディジタル・ビデオ装置が操作する更新データを前記第１プール内の前記ディジタル・ビデオ装置に送信するステップを含む、請求項２８のコンピュータ・プログラム装置。

【請求項３０】第２ディジタル・ビデオ装置が、第２セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第２ディジ

タル・ビデオ装置が、少なくとも第２プールを定義し、前記方法ステップがさらに、前記第２プール内のすべてのディジタル・ビデオ装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合は、前記第２プール内のディジタル・ビデオ装置に新しいセッション鍵を生成させるステップを含む、請求項２８のコンピュータ・プログラム装置。

【請求項３１】暗号漏洩されない装置の第１集合が、第１プールを定義し、暗号漏洩されない装置の第２集合が、第３プールを定義し、前記第１プールおよび前記第３プールのそれぞれが、暗号漏洩された装置を含まず、前記方法ステップがさらに、

前記第１プール内の装置に、前記第３プール内の前記装置のセッション鍵を用いてそのセッション鍵を置換させるステップを含む、請求項２８のコンピュータ・プログラム装置。

【請求項３２】前記ディジタル・ビデオ装置と組み合わされた、請求項２７のコンピュータ・プログラム装置。

【請求項３３】ディジタル処理装置によって読み取ることができるコンピュータ・プログラム記憶装置と、

ディジタル・ビデオ装置に少なくとも１つのディジタル番組を受信させ、提示させるための方法ステップを実行するために前記ディジタル処理装置によって実行可能な命令を含む、前記コンピュータ・プログラム記憶装置上のプログラム手段とを含み、前記方法ステップが、

ｉが１とＮを含む１からＮまでの整数であり、ｊが１とＭを含む１からＭまでの整数であり、「Ｎ」が鍵のＭ個の集合のそれぞれの装置鍵の数であるものとして、各セッション番号 x_i が第ｊ装置鍵 $S_{j,i}$ によって暗号化される暗号化されたセッション番号 x_i を含む、少なくとも次元「ｉ」および「ｊ」を有する行列によって表すことのできるセッション鍵ブロックを受信するステップと、

前記ディジタル・ビデオ装置に変数「ｉ」ごとに１つだけ割り当てられる複数の局所装置鍵にアクセスするステップと、

前記局所装置鍵を使用して前記セッション鍵ブロックからのセッション鍵を非暗号化するステップとを含む、コンピュータ・プログラム装置。

【請求項３４】前記方法ステップがさらに、

前記ディジタル・ビデオ装置が暗号漏洩された装置鍵を有しない場合には、前記ディジタル・ビデオ装置が第１セッション鍵を生成し、前記ディジタル・ビデオ装置が１つまたは複数の暗号漏洩された装置鍵を有する場合には、前記ディジタル・ビデオ装置が第２セッション鍵を生成し、前記第１セッション鍵だけが前記ディジタル番組の非暗号化に有用になるように、第ｉセッション番号を非暗号化するためにそれぞれの第ｉ局所装置鍵を使用するステップを含む、請求項３３のコンピュータ・プログラム装置。

【請求項３５】前記方法ステップがさらに、

更新データを受信するステップと、

１つまたは複数の新しい局所装置鍵を生成するために、前記更新データを操作するのに１つまたは複数の前記局所装置鍵を使用するステップとを含む、請求項３４のコンピュータ・プログラム装置。

【請求項３６】前記方法ステップがさらに、放送メッセージに応答して、前記セッション鍵を他の装置のセッション鍵によって置換するステップを含む、請求項３５のコンピュータ・プログラム装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、全般的にはデータ暗号化に関し、具体的には、許可されていないクローン受信器が番組を簡単に非暗号化できないようにする、放送番組の暗号化に関する。

【０００２】

【従来の技術】たとえば衛星またはケーブルによるペイ・パー・ビュー（pay-per-view）放送番組の、支払いを行わない顧客による許可されていない視聴およびコピーを防ぐために、そのような番組は、通常は暗号化される。許可された顧客には、その内部の非暗号化アルゴリズムに従って番組を非暗号化する、いわゆる「セット・トップ・ボックス」が与えられる。受信した番組に対する料金を許可された顧客に確実に請求するために、さまざまな課金方式が、セット・トップ・ボックスまたは他の顧客識別に結び付けられている。

【０００３】支払いを行わない多数の顧客に対するアクセスの阻止には有効であるが、このようなセット・トップ・ボックスは、比較的洗練されたクローニング技術を使用してクローンを作成し、販売することができ、これを購入した者は、そのクローンを使用して、本来はペイ・パー・ビューである番組を無料で視聴し、コピーすることができる。単独のクローン・ボックスがたまたま発見される可能性はあるが、大半は使用者の家庭で検出されないままになり、放送局の収入の損失につながる。

【０００４】この収入の損失は、ディジタル・コピーが完全なコピーであるから、特に家庭用ディジタル・ビデオ装置の発達に伴って、大きな問題になりつつある。実際、ディジタル・ビデオの発達は、「Ｆｉｒｅｗｉｒｅ」または「ＩＥＥＥ　１３９４」と称する新しいディジタル・バス標準規格の導入をもたらした。この標準規格は、ユーザのディジタル・テレビジョン、ディジタル・ビデオ・カセット・レコーダ（ＶＣＲ）、Digital Versatile Disk（ＤＶＤ）プレイヤーおよびセット・トップ・ボックスの間の相互接続を標準化するために提案されたものである。

【０００５】数百万台のセット・トップ・ボックスが同一の非暗号化アルゴリズム鍵を使用する可能性があるので、許可された装置のそれぞれに新しい非暗号化アルゴリズム鍵を個別に再プログラムすることは実現可能では

ない。実際、数百万台のペイ・パー・ビュー番組の家庭内非暗号化受信器を再プログラムするための実現可能な唯一の方法は、新しい暗号化アルゴリズム鍵を放送することであるが、許可されないクローンも、その新しい鍵の放送を受信し、古典的な放送暗号化の難問すなわち、許可されないクローンから権利を剥奪しながら、許可された受信器に新しい非暗号化鍵を効果的に再プログラミングするにはどうするかという問題につながる。本発明は、この問題に対処する。

【０００６】

【発明が解決しようとする課題】したがって、本発明の目的は、保護された番組放送のための暗号化システムを提供することである。本発明のもう１つの目的は、許可された家庭内ディジタル・ビデオ装置に暗号化更新を放送できる暗号化システムを提供することである。本発明のもう１つの目的は、許可された家庭内ディジタル・ビデオ装置の暗号化アルゴリズムを更新できると同時に、既知の許可されない装置が効果的に更新されないようにする暗号化システムを提供することである。本発明のもう１つの目的は、使いやすくコスト効率のよい、保護された番組放送のための暗号化システムを提供することである。

【０００７】

【課題を解決するための手段】１つまたは複数の放送番組を暗号化するためのシステムを開示する。このシステムには、複数のユーザ装置が含まれ、このユーザ装置のそれぞれに、装置鍵の集合から選択された複数のコンピュータ使用可能装置鍵が含まれる。セッション鍵ブロック・ジェネレータが、装置鍵の集合を用いて複数のセッション番号を暗号化して、セッション鍵ブロックを作り、少なくとも１つの装置が暗号漏洩された装置鍵を定義する暗号漏洩された装置であると判定される時に、少なくとも１つのセッション番号をダミー番号にすることができる。ダミー番号は、暗号漏洩された装置鍵によって暗号化され、その後、セッション鍵ブロックが、番組の非暗号化に使用するために送信される。各ユーザ装置にアクセスできる非暗号化モジュールは、その装置の装置鍵にアクセスして、セッション鍵ブロックとその装置のそれぞれの装置鍵とに基づいてセッション鍵を決定することができる。装置が暗号漏洩された装置鍵を有しないならば、このセッション鍵を使用してユーザ装置が番組を非暗号化できるが、暗号漏洩された装置鍵を有する装置では、結果的にダミー番号が非暗号化され、これを使用してセッション鍵が生成される。

【０００８】好ましい実施例では、装置鍵の集合を、鍵次元と集合次元を含む少なくとも２次元の行列によって表現できる。鍵次元では、それぞれが鍵インデックス変数「ｉ」によって表される「Ｎ」個の鍵位置が表され、集合次元では、それぞれが集合インデックス変数「ｊ」によって表される「Ｍ」個の集合が表され、各装置鍵を

表記$S_{j,i}$によって表すことができるようになっている。下で詳細を示す原理によれば、ある装置の２つの装置鍵が互いに同一の鍵インデックス変数「ｉ」を有することはない。

【０００９】好ましい実施例では、各セッション番号をx_iによって表せるように、鍵インデックス変数「ｉ」ごとにそれぞれのセッション番号が提供される。各セッション番号x_iは、セッション鍵ブロックを作るために、第ｉ鍵次元の装置鍵によってのみ暗号化される。さらに、各装置は、それぞれの第ｉ装置鍵$S_{j,i}$を使用して第ｉセッション番号を非暗号化して、暗号漏洩された装置鍵を有しないすべての装置が、少なくとも第１セッション鍵を生成し、暗号漏洩された装置鍵を有するすべての装置が、少なくとも第２セッション鍵を生成し、第１セッション鍵だけが番組の非暗号化に有用になる。

【００１０】特に好ましい実施例では、第１セッション鍵を生成する装置によって第１プールが定義され、第２セッション鍵を生成する装置によって第２プールが定義される。コンピュータ可読コード手段によって、第１プール内のすべての装置が暗号漏洩された装置でないかどうかを判定し、それらが暗号漏洩された装置でない場合には、暗号化された更新データがすべての装置に送られる。第１プールの装置だけが、この更新データを非暗号化でき、正しく操作することができる。これらの装置は、更新データを操作して、新しい装置鍵を生成する。さらに、コンピュータ可読コード手段によって、第２プール内のすべての装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合には、第２プールの装置に、異なる暗号漏洩された装置鍵を使用して新しいセッション鍵を生成させる。

【００１１】好ましい実施例のもう１つの特徴では、暗号漏洩されていない装置の第１の集合によって第１プールが定義され、暗号漏洩されていない装置の第２の集合によって第３プールが定義され、第１プールと第３プールのそれぞれに暗号漏洩された装置が含まれないようになっている。このような状況で帯域幅を節約するために、コンピュータ可読コード手段によって、第１プールの装置に、そのセッション鍵を第３プールの装置のセッション鍵で置換させる。上で示したシステムの機能を実行するコンピュータ実施される方法も開示される。

【００１２】もう１つの態様では、本発明は、放送データを暗号化するために本明細書に記載の発明的ステップに従ってプログラミングされた汎用コンピュータである。本発明は、ディジタル処理装置によって使用され、放送送信を暗号化するためにディジタル処理装置によって実行できる命令のプログラムを具体的に実施する製造品（機械構成要素）として実施することもできる。本発明は、ディジタル処理装置に本明細書に記載の発明的方法ステップを実行させるクリティカルな機械構成要素において実現される。

11

【００１３】本発明によれば、方法ステップに、ｉが１からＮまで（両端を含む）の整数、ｊが１からＭまで（両端を含む）の整数として、装置鍵$S_{j,i}$の行列にアクセスするステップが含まれる。本発明の原理によれば、「ｉ」は、この行列の鍵次元での位置を示す鍵インデックス変数であり、「ｊ」は、行列の集合次元での位置を示す集合インデックス変数であり、「Ｎ」は、鍵の「Ｍ」個の集合のそれぞれに含まれる装置鍵の数である。装置鍵の行列からの複数の装置鍵のそれぞれに、複数のディジタル・ビデオ装置が割り当てられ、このディジタル・ビデオ装置のそれぞれに、鍵インデックス変数「ｉ」ごとに１つの装置鍵だけが割り当てられる。さらに、複数のセッション番号x_i（ｉ＝１、…、Ｎ）が生成され、セッション番号x_iのそれぞれが、それぞれの鍵インデックス変数「ｉ」に対応する。セッション番号x_iのそれぞれを、すべての装置鍵$S_{j,i}$（ｊ＝１、…、Ｍ）を用いて暗号化して、セッション鍵ブロックを生成する。

【００１４】もう１つの態様では、少なくとも１つのディジタル番組を受信し、提示するように構成された、ディジタル・ビデオ装置のための非暗号化モジュールが開示される。このモジュールには、少なくとも次元「ｉ」および「ｊ」を有する行列によって表現されるセッション鍵ブロックを受信するためのコンピュータ可読コード手段が含まれる。セッション鍵ブロックには、暗号化されたセッション番号x_i（ｉ＝１、…、Ｎ）が含まれ、セッション番号x_iのそれぞれは、「ｊ」装置鍵$S_{j,i}$（ｊ＝１、…、Ｍ）によって暗号化される。本明細書で使用する「Ｎ」は、鍵の「Ｍ」個の集合のそれぞれに含まれる装置鍵の数である。コンピュータ可読コード手段は、複数の局所装置鍵にアクセスするが、変数「ｉ」に対して、ビデオ装置に１つの局所装置鍵だけが割り当てられることを理解されたい。また、コンピュータ可読コード手段には、局所装置鍵を使用してセッション鍵ブロックからセッション鍵を非暗号化するステップが含まれる。この非暗号化モジュールの機能を実行するコード手段を有するコンピュータ・プログラム製品も開示される。

【００１５】

【発明の実施の形態】まず図１を参照すると、保護された番組放送のためのシステム１０が示されている。「放送」とは、ケーブル、ワイヤまたは無線を介して多数のユーザに同時に番組を広く行き渡らせることを意味する。図示の特定のアーキテクチャでは、システム１０に、ライセンシング・エージェンシ・コンピュータすなわち、ディジタル処理装置（以下では、コンピュータと呼称する）１２が含まれる。所期の実施例の１つでは、コンピュータ１２は、図示のように米国ニューヨーク州アーモンクのInternational Business Machines Corporation（ＩＢＭ）が製造するパーソナル・コンピュータ

12

とするか、付随するIBM Network Stationを有する、ＡＳ４００などの商標の下で販売されるコンピュータを含む、任意のコンピュータとすることができる。または、コンピュータ１２は、ＵＮＩＸコンピュータ、ＯＳ／２サーバ、Ｗｉｎｄｏｗｓ　ＮＴサーバー、ＡＩＸ　３．２．５．が走行する主記憶１２８ＭＢのＩＢＭ　ＲＳ／６０００　２５０ワークステーション、またはＩＢＭ社のラップトップ・コンピュータとすることができる。

【００１６】コンピュータ１２には、暗号化モジュール１４が含まれ、この暗号化モジュール１４は、一連のコンピュータ実行可能命令としてコンピュータ１２内のプロセッサによって実行することができる。これらの命令は、たとえばコンピュータ１２のＲＡＭ内に常駐することができる。

【００１７】その代わりに、図２に示された、コード要素ＡないしＤを格納されたコンピュータ使用可能媒体１５Ａを有するコンピュータ・ディスケット１５などのコンピュータ可読媒体を用いるデータ記憶装置に命令を格納することができる。または、命令を、ＤＡＳＤアレイ、磁気テープ、通常のハード・ディスク装置、電子読取専用メモリ、光学記憶装置または他の適当なデータ記憶装置に格納することができる。本発明の実施例では、コンピュータ実行可能命令を、コンパイルされたＣ＋＋互換コードの複数の行とすることができる。

【００１８】実際、本明細書の流れ図には、コンピュータ・プログラム・ソフトウェアで実施された本発明のモジュールの構造が示されている。当業者であれば、これらの流れ図が、本発明に従って機能する、集積回路上の論理回路を含むコンピュータ・プログラム・コード要素の構造を示すものであることを諒解するであろう。明らかに、本発明は、その本質にかかわる実施態様において、ディジタル処理装置（すなわちコンピュータ）に図示のシーケンスに対応する機能ステップのシーケンスを実行するように指示する形のプログラム・コード要素を実行する機械構成要素によって実施される。

【００１９】図１からわかるように、暗号化モジュール１４は、放送番組供給源１６にアクセスし、実際に放送番組供給源１６の構成要素とすることができる。本発明によれば、暗号化モジュール１４は、放送番組供給源１６によって放送される１つまたは複数の番組の、ケーブル、ワイヤまたは無線の放送手段を介する複数のユーザのビデオ装置１８への保護された送信のためにこれらの番組を暗号化するのに使用される、暗号化データを提供する。

【００２０】図１には、ディジタル・テレビジョン２２およびディジタル・ビデオ・カセット・レコーダ（ＶＣＲ）２４を用いて通信することができるビデオ装置２０を有する第１の例のユーザが示されている。ビデオ装置２０には、セット・トップ・ボックス２６が含まれ、ディジタル・テレビジョン２２、ＶＣＲ２４およびセット

・トップ・ボックス２６は、バス２８を介して互いに通信する。したがって、最小限、ビデオ装置１８にはセット・トップ・ボックス２６またはその同等物が含まれる。図示されてはいないが、ビデオ装置２０には、Digital Versatile Disk（ＤＶＤ）プレイヤを含めることができる。所期の実施例の１つでは、バス２８は、いわゆる「Ｆｉｒｅｗｉｒｅ」または「ＩＥＥＥ　１３９４」ディジタル・ビデオ・データ・バスである。本発明では、ユーザのビデオ装置２０が家庭内ディジタル・システムであることが意図されているが、本明細書に開示される原理は、アナログの家庭内システムにも適用されることを理解されたい。

【００２１】上で述べた構成要素は、通常のディジタル・ビデオ構成要素とすることができるが、セット・トップ・ボックス２６には、本発明の新規の非暗号化モジュール３０が含まれる。たとえば上で述べたＦｉｒｅｗｉｒｅ応用などのいくつかの応用分野では、ディジタル・テレビジョン２２やＶＣＲ２４などの他の構成要素に非暗号化モジュール３０を含めることができる。非暗号化モジュール３０は、下で説明する論理に従って、暗号化モジュール１４からの暗号化データを使用して暗号化された放送番組を非暗号化するという点で、暗号化モジュール１４の相補物である。

【００２２】本発明によれば、各ユーザのビデオ装置１８には、複数の装置鍵が与えられる。装置鍵のそれぞれは、所定のビット・サイズの乱数であり、この好ましい実施例の所定のビット・サイズは、６４である。特定のビデオ装置１８の装置鍵は、そのそれぞれの非暗号化モジュール３０からアクセスでき、システム１０で使用される装置鍵全体の集合は、まもなく開示する目的のために、暗号化モジュール１４からアクセス可能である。さらに、ライセンシング・エージェンシは、それぞれのビデオ装置１８に与えられるそれぞれの装置鍵の部分集合のリストを保存する。

【００２３】図３は、システム１０の装置鍵全体の集合を表す、２次元の行列３２を示す図である。この図では、装置鍵が記号$S_{j,i}$によって表され、ｉは１からＮまでの整数（両端を含む）、ｊは１からＭまでの整数（両端を含む）である。本発明の原理によれば、「ｉ」は、行列３２の鍵次元３４での位置を示す鍵インデックス変数であり、「ｊ」は、行列３２の集合次元３６での位置を示す集合インデックス変数である。

【００２４】さらに、「Ｎ」は、鍵の「Ｍ」個の集合のそれぞれに含まれる装置鍵「Ｓ」の数である。言い換えれば、「Ｎ」は、鍵次元３４のカーディナリティ（cardinarity）であり、「Ｍ」は、集合次元３６のカーディナリティである。図３では、鍵の集合「Ｓ」が７つあり（すなわちＭ＝７）、集合のそれぞれに８つの鍵が含まれる（すなわちＮ＝８）。しかし、開示を簡潔明瞭にするために図３には５６個の鍵だけが示されているが、好ましい実施例では３２個の鍵の集合のそれぞれに１２８個の鍵があることを理解されたい。さらに、これより大きいまたはこれより小さい鍵次元３４および集合次元３６のカーディナリティの値が、本発明の範囲に含まれることを理解されたい。

【００２５】本発明の意図によれば、各ユーザのビデオ装置１８には、ライセンシング・エージェンシによって行列３２から選択された鍵「Ｓ」が割り当てられる。たとえば、第１のユーザのビデオ装置２０に、鍵$S_{3,1}$、$S_{5,2}$、$S_{1,3}$、$S_{1,4}$、$S_{6,5}$、$S_{4,6}$および$S_{8,7}$が割り当てられる。どの場合でも、各ユーザのビデオ装置１８には、「Ｎ」個の装置鍵が割り当てられ、各ビデオ装置１８には、鍵インデックス変数「ｉ」ごとに装置鍵「Ｓ」が１つだけ割り当てられる。しかし、装置が第ｉ位置のそれぞれについて１つの装置鍵を含まない実施態様は、本発明の範囲内である。どの場合でも、ビデオ装置１８は、鍵インデックス次元での同一位置で２つの鍵を知ることはない。多数の装置の装置鍵がオーバーラップする可能性はあるが、ビデオ装置１８が、他の装置と正確に同一の装置鍵「Ｓ」を有しないことが好ましい。

【００２６】ビデオ装置１８の装置鍵「Ｓ」が割り当てられ、ビデオ装置１８が使用されるようになった後に、ディジタル・ビデオ番組を含む番組を、図４に示された論理を使用して放送番組供給源１６からさまざまなユーザのビデオ装置１８へ保護された状態で送信できる。処理はブロック３８から開始され、「Ｎ」個のセッション番号「x_i」がランダムに生成される。各セッション番号は長さ「ｌ」を有する。好ましい実施例の１つでは、各セッション番号「ｘ」の長さ「ｌ」は、６４ビットである。その後、ブロック４０で、各セッション番号x_iを、ｉ番目の装置鍵$S_{j,i}$（ｊ＝１、…、Ｍ）ごとに１回ずつ、「Ｍ」回暗号化して、セッション番号x_iの「Ｍ」版を作る。

【００２７】ブロック４０の結果が、図５に示された行列４２である。行列４２では、各セッション番号x_iの複数の暗号化された版Ｅ（x_i、$S_{j,i}$）を含むセッション鍵ブロックが定義されている。したがって、少なくともブロック４０の論理によって、セッション鍵ブロック・ジェネレータが確立される。当業者であれば、図５に示された行列４２のサイズが、図３に示された行列３２のサイズと同一であることを諒解できる。

【００２８】図４のブロック４４に移ると、セッション鍵ブロックが、放送データ・ストリームの暗号化番組の先頭に挿入される。これに関して、図６に、番組の暗号化に使用され、その結果、その番組の非暗号化に使用できるセッション鍵を計算するようにビデオ装置１８に指示するための１つの特定のメッセージ４６の形式を示す。

【００２９】図示された特定のメッセージ４６には、メッセージのタイプを識別するメッセージ識別フィールド

４８と、それに続く３２ビットの更新世代番号フィールド５０が含まれる。各ビデオ装置１８は、更新世代番号が、特定のビデオ装置１８の更新と一致するかどうかを判定し、そうである場合には、ビデオ装置１８はそのメッセージを検討する。そうでない場合には、ビデオ装置１８はそのメッセージを無視する。下で説明するように、許可されない装置が存在する場合、システム１０は、装置鍵「Ｓ」を更新し、更新世代番号は、装置の鍵が更新された回数を表す。

【００３０】更新世代番号フィールド５０の次に、上で述べたセッション鍵ブロックを含むセッション鍵ブロック・フィールド５２がある。暗号化プログラムが、メッセージの本体５４を確立する。

【００３１】適当な更新世代番号の装置がセッション鍵計算メッセージであるメッセージ４６を受信した時には、その非暗号化モジュール３０が、図４のブロック５６に示された論理を呼び出す。ブロック５６では、ビデオ装置１８が、セッション鍵ブロックからセッション鍵を非暗号化して、放送番組を非暗号化する。これを行うために、ビデオ装置は、その装置鍵$S_{j,i}$（ｉ＝１、…、Ｎ）を使用して、それぞれのｉ番目のセッション番号x_iを非暗号化する。各ビデオ装置は、たとえばセッション番号のすべてに対してＸＯＲ演算を使用することなどによって、非暗号化されたセッション番号のすべてをハッシュして、その後にブロック５８で放送中の共通鍵として使用されるセッション鍵を作る。したがって、ビデオ装置１８は、同一のセッション鍵を計算するが、異なる装置鍵「Ｓ」を使用してそのセッション鍵を得る。

【００３２】本発明では、ビデオ装置１８のうちの１つが、いわゆる「著作権侵害者」によって取得され、その著作権侵害者が装置鍵と共にビデオ装置のクローンを作成して、望ましくないことに番組を受信し、非暗号化できる１つまたは複数の許可されない装置を作る可能性があることが認識されている。ライセンシング・エージェンシがこのような許可されない装置について学ぶことは可能である。本発明が対処する課題は、許可されない装置が読み取れない放送メッセージを許可された装置に送信することである。これを行うために本発明によって実行される論理を、図７に示す。

【００３３】判断ブロック６０で、ビデオ装置１８が暗号漏洩されたものであるかどうか、すなわち、許可されない装置が存在するかどうかを判定する。存在しない場合、処理は状態６２で終了する。この状況の下では、図４に示された論理が番組の放送に使用されると理解される。

【００３４】その一方で、ライセンシング・エージェンシが、少なくとも１つのビデオ装置１８が暗号漏洩されたものであると判定した時には、エージェンシは、暗号漏洩された装置に割り当てられた装置鍵の部分集合にアクセスし、処理は、判断ブロック６０からブロック６４に進んで、暗号漏洩された装置に割り当てられた特定の装置鍵$S_{j,i}$が存在する、暗号漏洩された装置の少なくとも１つの鍵位置、たとえば第ｉ鍵位置を識別する。開示を明瞭にするために、下の説明では暗号漏洩された装置の単一の鍵位置だけが選択されると仮定することを理解されたい。しかし、下で説明する原理は、複数の装置鍵位置の選択とそれらの同時処理に適用できる。

【００３５】ブロック６６に移ると、この論理は、上で述べた原理に従う、ｉ以外のすべてのセッション番号x_{non-i}の、ｊ以外のすべて（暗号漏洩されたビデオ装置１８の装置鍵$S_{j,i}$に対して）の対応する装置鍵$S_{non-j,non-i}$を用いる暗号化を想定したものである。また、ブロック６８では、第ｉセッション番号x_iが、ｊ以外のすべての装置鍵$S_{non-j,i}$を用いて暗号化される。これによって、暗号化について残された唯一のセッション・ブロック行列要素として、選択された暗号漏洩された装置鍵$S_{j,i}$が存在する位置のセッション番号が残される。

【００３６】したがって、ブロック７０で、選択された暗号漏洩された$S_{j,i}$を使用してある数字が暗号化されるが、この数字は、第ｉセッション番号x_iではなく、ダミー番号「ｙ」である。その結果、図８に示されたセッション鍵ブロック７２が、ブロック７０の後に作られ、図７のブロック７４で送信される。図からわかるように、図８のセッション鍵ブロック７２は、実質的に図５に示された行列４２と同一であり、図４の論理で生成されるが、図８のセッション鍵ブロック７２に、ダミー番号「ｙ」を暗号化したものを表すダミー位置７６が含まれる点が異なる。

【００３７】これで、ビデオ装置１８のほとんどが、ブロック６４で選択された第ｉ位置を占める暗号漏洩された装置の選択された暗号漏洩された装置鍵$S_{j,i}$を有すると期待されず、すべてのセッション番号「ｘ」を成功裡に非暗号化し、したがって、セッション鍵を成功裡に計算することが理解される。対照的に、暗号漏洩された装置は、第ｉセッション番号x_iを非暗号化するのではなく、ダミー番号「ｙ」を非暗号化する。その結果、正しいセッション鍵は、ダミーでないセッション番号x_i（ｉ＝１、…、Ｎ）のすべてを組み合わせることによってのみ決定できるので、暗号漏洩された装置は、正しいセッション鍵を計算できず、したがって、番組を含む付随メッセージを非暗号化することができない。

【００３８】特定の選択された暗号漏洩された装置鍵$S_{j,i}$をたまたま使用し、その結果、暗号漏洩された装置と同様に、正しいセッション鍵を計算できない許可された装置に関しては、許可された装置のどれもが、他の許可された装置と正確に同一の装置鍵の組合せを有しないことを想起されたい。これを念頭において、許可された装置のすべてに有効なセッション鍵が与えられるまで、

17

上で説明した手順を、暗号漏洩された装置の１つまたは複数のｉ以外の装置鍵$S_{j,non-i}$について繰り返す。

【００３９】後続の繰り返しを行う際には、新しいセッション鍵ブロックは条件的に作られる。具体的に言うと、既存のセッション鍵が、図７に示された手順の開始の前に存在した鍵である場合に限って、新しいセッション鍵ブロックが付随するメッセージによって、装置が新しいセッション鍵を計算するように指示される。当業者であれば、繰り返しのそれぞれの後に、追加の許可された装置が正しいセッション鍵を計算でき、暗号漏洩された装置とそのクローンだけが正しいセッション鍵を有しない状態になるまで、「事情を知らない」装置のプールが徐々に小さくなることを理解するであろう。

【００４０】条件付きセッション鍵計算メッセージ７８のフォーマットの例を、図１０に示す。条件付きセッション鍵計算メッセージ７８には、メッセージのタイプを識別するメッセージ識別フィールド８０と、その後の認証フィールド８２が含まれる。認証フィールド８２には、所定のセッション鍵を用いなければ非暗号化できない認証データが含まれる。ビデオ装置１８が、認証データの非暗号化の際に所定のコード、たとえば、単語「ＤＥＡＤＢＥＥＦ」を生成する場合、その装置は条件付きセッション鍵計算メッセージ７８を検討する。そうでない場合には、その装置はこのメッセージを無視する。認証フィールド８２の次に、図６に関連して上で説明したように使用される更新世代番号フィールド８４があり、その後に新規のセッション鍵ブロック・フィールド８６がある。

【００４１】望むならば、上の手順を使用して、許可された装置と暗号漏洩された装置を区別する鍵位置を複数選択することによって、複数の暗号漏洩された装置を分離することができる。どの場合でも、暗号漏洩された装置を分離した後に、許可された装置の装置鍵を、暗号化鍵として正しいセッション鍵を使用して更新することができる。更新のたびに、上で述べた更新サイクル番号が１つ増やされる。

【００４２】図９は、前の段落で述べた論理の詳細を示す図である。処理はブロック８８から開始され、共通のセッション鍵（その鍵が有効であるかどうかに無関係に）を有する装置のプールごとに「ＤＯ」ループに入る。判断ブロック９０では、テスト中のプールに含まれる装置の特定の装置鍵を検討することによって、すべての装置が暗号漏洩された（図では「不正」と表記）装置であるかどうかを判定する。そうである場合には、この論理は、不正装置とこれ以上通信せずに状態９２で終了する。そうでない場合には、この論理は判断ブロック９４に進んで、テスト中のプールに含まれる装置が「正規」（すなわち許可された装置）と不正の混合であるかどうかを判定する。そうである場合には、前に述べたようにこの論理はブロック９６に進んで、図７に示された

18

処理を使用し、もう１つの暗号漏洩された鍵を使用してダミー変数「ｙ」を暗号化し、図１０の条件付きセッション鍵計算メッセージを使用して図８のセッション鍵ブロック７２を送るという処理を反復する。その後、この処理は、ブロック８８にループ・バックして、ブロック９６からもたらされたより少数の装置のプールを使用して、次の反復についてテストを行う。

【００４３】その一方で、判断ブロック９４で、テスト中のプールに含まれるすべての装置が許可された（「正規」の）装置であると判定された場合、この論理は判断ブロック９８に進んで、正規の装置だけを有するプールが複数存在するかどうかを判定する。そうである場合には、帯域幅を節約するために、この論理はブロック１００に進んで、１つのプールにセッション鍵変更メッセージを送信して、そのセッション鍵を他の「正規」プールのセッション鍵と交換し、これによって、両方のプールの装置鍵を更新する前に両方のプールがセッション鍵を変更する必要をなくす。

【００４４】図１１は、図１０に関連して上で説明した原理による、メッセージ識別フィールド１０４と認証フィールド１０６を含むセッション鍵変更メッセージ１０２を示す図である。セッション鍵変更メッセージ１０２には、セッション鍵変更メッセージ１０２を認証する装置のプールによって使用されるセッション鍵を含む新規鍵フィールド１０８も含まれる。

【００４５】望むならば、ライセンシング・エージェンシは、下で説明するいわゆる「潜伏」攻撃の威力を下げるために、セッション鍵を保持される「正規」プールの独自の装置鍵をまず更新することができる。具体的に言うと、本発明によって認識されるように、著作権侵害者は、第１の暗号漏洩された装置のクローンを大量に作成し、その装置は、クローンを大量に作成されているので比較的簡単に発見できるが、この著作権侵害者が異なる鍵を秘密にされた第２の暗号漏洩された装置を保持し、これによって、第１の暗号漏洩された装置のクローンを更新するための更新された鍵を学習しようとして検出を逃れる可能性がある。したがって、本発明の論理を、図９のブロック１００から、潜伏攻撃の疑いがあるかどうかを判定する判断ブロック１１０に移動することができる。潜伏攻撃の疑いがある場合、この論理はブロック１１２に進んで、潜伏中の暗号漏洩された装置を分離するために、すべての「正規」プールについて図７の論理を実行する。これは、各プールが、そのプールの装置によって使用されない鍵のための鍵更新データから、余分な鍵更新データを与えられていないことを確認することによって行われる。したがって、潜伏中の装置は、広く配布されたクローン装置のための鍵更新データの一部を学ぶことができなくなる。

【００４６】ブロック１１２から、または潜伏攻撃の疑いがない場合に判断ブロック１１０から、この論理は、

19

最終的にブロック１１４に進み、各「正規」プールの装置の装置鍵を、そのプールのセッション鍵と図１２に示された装置鍵更新メッセージ１１６を使用して更新する。

【００４７】図からわかるように、図１２の装置鍵更新メッセージ１１６には、メッセージのタイプを識別するメッセージ識別フィールド１１８と、その後の、メッセージの残りの暗号化されたバイト数を示す１６ビットの通信長フィールド１２０が含まれる。通信長フィールド１２０の後には、上で原理を開示した認証フィールド１２２と更新世代番号フィールド１２４がある。

【００４８】更新世代番号フィールド１２４の次に、開始鍵フィールド１２６がある。本発明によれば、開始鍵フィールド１２６は、最初に更新される装置鍵の「ｉ」および「ｊ」の値を示す。

【００４９】次に、装置鍵更新メッセージ１１６には、更新される鍵ごとに８バイトを含む更新データ・フィールド１２８が含まれる。更新データのどれかに、特定のビデオ装置１８に関連するデータが含まれる場合、そのビデオ装置は、第ｉ位置での更新データと第ｉ位置の以前の装置鍵との連結に対する組合せ関数を計算する。好ましい実施例では、組合せ関数はＸＯＲであるが、以前の鍵と更新データの両方を使用する関数であれば、どれでも適しており、本発明の範囲に含まれる。その結果が、特定のビデオ装置１８の新しい第ｉ装置鍵である。ライセンシング・エージェンシは、古い装置鍵と更新データの両方を知っているので、ビデオ装置１８の新しい装置鍵も知っている。本明細書で認識されているように、ライセンシング・エージェンシに未知の不正装置は、このステップの結果として、すでに知っているもの以外にはなにも学ぶことはない。

【００５０】上のメッセージは、他の応用分野に適するようにフォーマットすることができることを理解されたい。特に重要な応用分野が、コピー・プロテクションである。ハリウッド映画などの放送番組は、「コピー不可」または「１回のみコピー可能」と指定される。ＶＣＲなどの合法的に動作する装置が、この制限を尊重することが望ましい。本発明は、次のように使用される。正しく動作することが知られている合法的な装置は、上で述べた形で装置鍵を付与される。放送と共に送信されるセッション鍵ブロックは、セット・トップ・ボックスから家庭のシステムの他の構成要素にそのまま渡される。セット・トップ・ボックスは、セッション鍵を使用して映画を暗号化（または再暗号化）し、他の装置は、本発明を使用してそれを非暗号化する。装置鍵を有する合法的な装置だけが、映画を表示または録画することができ、不正コピーは不可能である。

【００５１】同様に、合法的な装置の鍵をクローン複製された非合法な記録装置が作られる場合、本発明を使用して、合法的な、クローン複製されたものでない装置だ

20

けを更新することができる。好ましい実施例では、装置は、Ｆｉｒｅｗｉｒｅバスによって接続され、本発明は、「ｃｏｐｙ－ｏｎｃｅ（１回のみコピー可能）」内容が保護される制限認証方法として既知の機能を提供する。この認証方法を使用するビデオ装置１８は、ディジタル・ビデオ・カセット・レコーダ（ＤＶＣＲ）と一体型ディジタル・ビデオ・カメラである。通常、他のすべての装置は、ＤＶＣＲまたは一体型ディジタル・ビデオ・カメラに接続された時だけこの認証方法を使用する。ｃｏｐｙ－ｏｎｃｅ内容は、セッション鍵ブロックの後に放送される。セット・トップ・ボックスは、ＤＶＣＲにセッション鍵ブロックを送り、このセッション鍵ブロックによって、両側での共通鍵の計算が容易になる。

【００５２】ライセンシング・エージェンシが更新サイクルの実行を希望する時には、すべてのｃｏｐｙ－ｏｎｃｅ放送の前に、更新命令を付加しなければならない。この更新命令は、レコーダが電源を切断され、番組を受信していない場合に備えて、単独の番組のためだけに送信してはならず、数週間にわたって繰り返されなければならない。さらに、１日１回（たとえば午後３時）全更新サイクルの全体の活動記録を放送しなければならない。したがって、長期間電源を切断されていた「リップ・バン・ウィンクル」装置を、２４時間以内に最新レベルにすることができる。実際、更新活動記録をより頻繁に放送する「更新チャネル」を設けることができる。

【００５３】更新の後に、セッション鍵が旧世代である記録された素材は、もはや機能しなくなる。しかし、これは必ずしも望ましくない状態ではない。というのは、「ｃｏｐｙ－ｏｎｃｅモード」の目的が、「タイム・シフト」（別の時に再生するために番組を記録する）用であり、そのような形で記録された映画が長期間存続することは、内容所有者の観点からは望ましくないからである。

【００５４】それでも、新しい更新サイクルの先頭で、記録の寿命が短すぎる瞬間が存在する可能性がある。これを考慮に入れるために、ライセンス・エージェンシは、新しい更新サイクルを予想することができ、新しい更新サイクルの直前に、現在の世代のセッション鍵ブロックと、まだ配布されていない次の世代のセッション鍵ブロックの両方を送信することができる。

【００５５】「Ｆｉｒｅｗｉｒｅ」バス応用例に加えて、本発明では、本明細書に開示された原理を、衛星システム、ケーブル・テレビジョン・システム、ＤＶＤムービー、および、インターネット上または他の放送配布媒体を介する他の広く配布されているマルチメディア内容を含む他の放送応用分野に適用できることが認識されている。

【００５６】下に、上で開示した発明を実施するコンピュータ擬似コード・リスティングを示す。

【００５７】本明細書で図示され、詳細に説明された特

定の「暗号漏洩された受信装置の存在下で放送番組を暗号化するためのシステム」は、本発明の上述の目的を完全に達成することができるが、これは本発明の好ましい実施例であり、したがって、本発明によって広義に意図される目的を代表するものであり、本発明の範囲は、当

業者に明白になるであろう他の実施例を完全に包含し、本発明の範囲は、請求項以外の何物によっても制限されないことを理解されたい。

【００５８】

【表１】

```
/*
サイズに関する前提：

  以下のルーチンがすでに存在する。これらのルーチンは、このプロトコルの
  他の動作のために必要である。このサイジングを行う際に使用される具体的
  な前提を示す。
*/

void *read();  /*  バスから読み取り、現在のバッファを返す。このルーチン
                   は、データが返されるまでブロックする。バス上のブロックサ
                   イズは、最大５１２バイトである。バッファ管理は、このルー
                   チンの下位にあり、おそらくピンポン・バッファと別のスレッ
                   ドが使用される。コマンドがバッファ境界をまたぐことはない
                   と仮定する。バンド外信号（たとえばバス・リセット）は、全
                   く返されない。その代わりに、プロセッサ全体がリセットされ
                   る。バッファは、必ずlong *に位置合せされる。 */
void hash(unsigned long *from, unsigned long *to, short length);
                /* メモリ内の所与の区域をハッシュし、ハッシュをto区域にセッ
                   トする。lengthはバイト単位である。 */
void decrypt(unsigned long *from, unsigned long *to, short length,
                 unsigned long *key);
                /* 所与のバッファを非暗号化する。fromとtoが同一の場合、その
                   場所で非暗号化する。lengthはバイト単位である。keyは必ず８バ
                   イト（２つのlong）である。非暗号化処理は、一般に、パスに追
                   従できる（鍵が頻繁に変更される場合を除く）。 */
```

【表２】

23 24

```
#define ntohl(v) (v)
        /* バス上の数値をプロセッサ固有形式に変換する。これによって
        、たとえばビッグ・エンディアンがリトル・エンディアンに変換
        される。このサイジングでは無処理と仮定する。 */

// NVRAM
static unsigned long deviceKeys[32];
static unsigned long globalGeneration;

// ROM; must be different for each device
static const unsigned short keyPosition[33];
        /* 装置鍵の各ワード内のセッション鍵に含まれるワード。トリック
        ：第３３位置は、必ず鍵の総数より大きいので、末尾を超えたかどう
        かを検査する必要はない。 */

void calculateSessionKey(
  long sessionKey[2], // ルーチンによって書き込まれる
  unsigned long *buf) // バッファの現在の内容
  unsigned long X[32];
  unsigned short word; // バッファの先頭にあるunsigned longの鍵の位置
  short i = 0; // 鍵ワードのインデックス

  unsigned long gen = ntohl(buf[0]);

  gen >>= 8;
```

【表３】

25 26

```
  for (word = -1; word < 16*256*2 - 2; word += 128) {
    for (; word + 128 > keyPosition[i]; i++) {
      X[i] = ntohl(buf[keyPosition[i] - word]);
    }
    buf = read();
  }

  if (gen == globalGeneration) {

    sessionKey[0] = sessionKey[1] = 0;

    for (i=0; i < 32; i += 2) {
      unsigned long t[2];
      decrypt(&X[i], t, 8, &deviceKeys[i]);
      sessionKey[0] ^= t[0];
      sessionKey[1] ^= t[1];
    }
  }
}

void newSessionKey(
  long sessionKey[2], // DEADBEEFが見つかった場合にこのルーチンでセッ
                      トされる
  unsigned long *buf) // バッファの現在の内容
{
```

【表４】

27 28

```
  decrypt(&buf[1], &buf[1], 16, sessionKey);

  if (buf[1] == 0xDEADBEEF) {
    sessionKey[0] = buf[2];
    sessionKey[1] = buf[3];
  }
}

void updateDeviceKeys(
  long sessionKey[2], // 現在のセッション鍵、変更されない
  unsigned long *buf) // バッファの現在の内容
{
  unsigned long X[32];
  unsigned short word; // 長さ；現在のバッファを含むunsigned longの数
  short i = 0; // 鍵番号のインデックス

  unsigned long gen = ntohl(buf[0]);
  unsigned long t   = ntohl(buf[1]);
  unsigned long deadBeef;
  unsigned short start = (unsigned short) (t >> 16); // 先頭の鍵番号
  unsigned short len   = (unsigned short) (t); // 鍵の数

  gen >>= 8;

  decrypt(&buf[2], &buf[2], 504, sessionKey);
```

【表５】

29 30

```
deadBeef = buf[2];

for (word = start << 1 - 3; ;) {
   for (; word + 128 > keyPosition[i]; i++) {
      if (word <= keyPosition[i]) {
         X[i] = ntohl(buf[keyPosition[i] - word]);
      }
   }
   word += 128;
   if (word >= (start + len) << 1 - 3) {
      break;
   }
   buf = read();
   decrypt(buf, buf, 512, sessionKey);
}

if (deadBeef == 0xDEADBEEF) {

   globalGeneration = gen;

   for (i= start >> 8; i <= (start + len) >> 8; i ++) {
      unsigned long t[4];
      short n = keyPosition[i << 1] >> 1;
      if (n < start || n - start >= len) {
         continue;
```

【表６】

```
31                                                    32
            }
            t[0] = deviceKeys[i];
            t[1] = deviceKeys[i+1];
            t[2] = X[i];
            t[3] = X[i+1];
            hash(t, &deviceKeys[i], 16);
        }
    }

    int main(int argc, char *argv[])
    {
       return 0;
    }

    void *read()
    {
       return 0;
    }

    void hash(unsigned long *from, unsigned long *to, short length)
    {
    }
```

【表７】

```
void decrypt(unsigned long *from, unsigned long *to, short length,
  unsigned long *key)
{
}
```

【００５９】まとめとして、本発明の構成に関して以下の事項を開示する。

【００６０】（１）装置鍵の集合から選択された複数のコンピュータ使用可能装置鍵をそれぞれが含む複数のユーザ装置と、セッション鍵ブロックを作るために装置鍵の前記集合を用いて複数のセッション番号を暗号化するための少なくとも１つのセッション鍵ブロック・ジェネレータであって、前記装置のうちの少なくとも１つが暗号漏洩された装置鍵を定義する暗号漏洩された装置であると判定された時に前記セッション番号のうちの少なくとも１つがダミー番号になり、前記ダミー番号が少なくとも１つの暗号漏洩された装置鍵によって暗号化され、前記セッション鍵ブロックが番組の非暗号化に使用するために送信される、前記少なくとも１つのセッション鍵ブロック・ジェネレータと、各ユーザ装置にアクセスでき、前記セッション鍵ブロックおよび前記装置のそれぞれの前記装置鍵に基づいてセッション鍵を判定するために前記装置の前記装置鍵にアクセスする非暗号化モジュールであって、前記セッション鍵が、前記装置が前記セッション鍵の生成に前記ダミー番号を使用しない限り、前記番組を非暗号化するためにユーザ装置によって使用可能である、前記非暗号化モジュールとを含む、１つまたは複数の放送番組を暗号化するためのシステム。

（２）装置鍵の前記集合が、鍵次元および集合次元を含む少なくとも２次元の行列によって表され、前記鍵次元が、鍵インデックス変数「ｉ」によってそれぞれが表される「Ｎ」個の鍵位置を表し、前記集合次元が、集合インデックス変数「ｊ」によってそれぞれが表される「Ｍ」個の集合を表し、各装置鍵を$S_{j,i}$によって表すことができる、上記（１）のシステム。

（３）ある装置の２つの装置鍵のいずれもが、互いに同一の鍵インデックス変数「ｉ」を有しない、上記（２）のシステム。

（４）各セッション番号をx_iによって表すことができるように、鍵インデックス変数「ｉ」ごとにそれぞれのセッション番号が設けられ、各セッション番号x_iが、前記セッション鍵ブロックを作るために第ｉ鍵次元の装置鍵によってのみ暗号化される、上記（３）のシステ

ム。

（５）暗号漏洩された装置鍵を有しないすべての装置が、少なくとも第１セッション鍵を生成し、暗号漏洩された装置鍵を有するすべての装置が、少なくとも第２セッション鍵を生成し、第１セッション鍵だけが前記番組の非暗号化に有用になるように、各装置が、前記第ｉセッション番号を非暗号化するためにそれぞれの第ｉ装置鍵$S_{j,i}$を使用する、上記（４）のシステム。

（６）前記第１セッション鍵を生成する装置が、少なくとも第１プールを定義し、前記第２セッション鍵を生成する装置が、少なくとも第２プールを定義し、前記システムがさらに、前記第１プール内のすべての装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に前記第１プール内の前記装置に、前記装置が新しい装置鍵を生成するために操作する更新データを送信するためのコンピュータ可読コード手段を含む、上記（５）のシステム。

（７）前記第２セッション鍵を生成する装置が、少なくとも第２プールを定義し、前記システムがさらに、前記第２プール内のすべての装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合に前記第２プール内の装置に新しいセッション鍵を生成させるためのコンピュータ可読コード手段を含む、上記（５）のシステム。

（８）暗号漏洩されない装置の第１集合が、第１プールを定義し、暗号漏洩されない装置の第２集合が、第３プールを定義し、前記第１プールおよび前記第３プールのそれぞれが、暗号漏洩された装置を含まず、前記システムがさらに、前記第１プール内の装置に、そのセッション鍵を前記第３プール内の装置の前記セッション鍵によって置換させるためのコンピュータ可読コード手段を含む、上記（５）のシステム。

（９）ディジタル番組を放送するためにこれを暗号化するためのコンピュータ使用可能コード手段を有するコンピュータ使用可能媒体を含むデータ記憶装置を具備するコンピュータにおいて、前記コンピュータ使用可能コード手段が、ｉが１とＮを含む１からＮまでの整数であり、ｊが１とＭを含む１からＭまでの整数であり、「ｉ」が装置鍵$S_{j,i}$の行列の鍵次元での位置を示す鍵次元インデックス変数であり、「ｊ」が前記行列の集合次元での位置を示す集合インデックス変数であり、「Ｎ」が鍵のＭ個の集合のそれぞれの装置鍵の個数であるものとして、前記装置鍵$S_{j,i}$の行列にアクセスするためのコンピュータ可読コード手段と、鍵インデックス変数「ｉ」ごとに各ディジタル・ビデオ装置に１つの装置鍵だけが割り当てられるように、複数の前記ディジタル・ビデオ装置に装置鍵の前記行列からそれぞれの複数の装置鍵を割り当てるためのコンピュータ可読コード手段と、ｉが１とＮを含む１からＮまでの整数であるものとして、各セッション番号x_iがそれぞれの鍵インデックス変数「ｉ」に対応するように複数の前記セッション番号x_iを生成するためのコンピュータ可読コード手段と、ｊが１とＭを含む１からＭまでの整数であるものとして、セッション鍵ブロックを生成するために、すべての装置鍵$S_{j,i}$を用いて各セッション番号x_iを暗号化するためのコンピュータ可読コード手段とを含む、コンピュータ。

（１０）前記ディジタル・ビデオ装置のうちの１つまたは複数が暗号漏洩された装置であるかどうかを判定するためのコンピュータ可読コード手段と、前記暗号漏洩された装置の少なくとも１つの暗号漏洩された装置鍵によって暗号化されるダミー番号として、前記セッション番号のうちの少なくとも１つを作るためのコンピュータ可読コード手段とをさらに含む、上記（９）のコンピュータ。

（１１）第１ディジタル・ビデオ装置が、第１セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第１ディジタル・ビデオ装置が、少なくとも第１プールを定義し、第２ディジタル・ビデオ装置が、第２セッション鍵を生成するために前記セッション鍵のうちの少なくとも一部を非暗号化し、前記第２ディジタル・ビデオ装置が、少なくとも第２プールを定義し、前記コンピュータがさらに、前記第１プール内のすべての装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に前記第１プール内の前記ディジタル・ビデオ装置に、前記ディジタル・ビデオ装置が新しい装置鍵を生成するために操作する更新データを送信するためのコンピュータ可読コード手段を含む、上記（１０）のコンピュータ。

（１２）第２ディジタル・ビデオ装置が、第２セッション鍵を生成するために前記セッション鍵ブロックの少なくとも一部を非暗号化し、前記第２ディジタル・ビデオ装置が、少なくとも第２プールを定義し、前記コンピュータがさらに、前記第２プール内のすべての装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合に前記第２プール内の装置に新しいセッション鍵を生成させるためのコンピュータ可読コード手段を含む、上記（１０）のコンピュータ。

（１３）暗号漏洩されない装置の第１集合が、第１プールを定義し、暗号漏洩されない装置の第２集合が、第３プールを定義し、前記第１プールおよび前記第３プールのそれぞれが、暗号漏洩された装置を含まず、前記コンピュータがさらに、前記第１プール内の装置に、そのセッション鍵を前記第３プール内の前記装置の前記セッション鍵によって置換させるためのコンピュータ可読コード手段を含む、上記（１０）のコンピュータ。

（１４）前記ディジタル・ビデオ装置と組み合わされた、上記（９）のコンピュータ。

（１５）ｉが１とＮを含む１からＮまでの整数であり、ｊが１とＭを含む１からＭまでの整数であり、「Ｎ」が

鍵のＭ個の集合のそれぞれの装置鍵の数であるものとして、それぞれが「ｊ」装置鍵$S_{j,i}$によって暗号化されるセッション番号x_iを含み、少なくとも次元「ｉ」および「ｊ」を有する行列によって表現できるセッション鍵ブロックを受信するためのコンピュータ可読コード手段と、変数「ｉ」ごとに１つだけディジタル・ビデオ装置に割り当てられる複数の局所装置鍵にアクセスするためのコンピュータ可読コード手段と、前記局所装置鍵を使用して前記セッション鍵ブロックからのセッション鍵を非暗号化するためのコンピュータ可読コード手段とを含む、少なくとも１つのディジタル番組を受信し、提示するために構成された前記ディジタル・ビデオ装置のための非暗号化モジュール。

（１６）さらに、前記ディジタル・ビデオ装置が暗号漏洩された装置鍵を有しない場合に、前記ディジタル・ビデオ装置が第１セッション鍵を生成し、前記ディジタル・ビデオ装置が１つまたは複数の暗号漏洩された装置鍵を有する場合に、前記ディジタル・ビデオ装置が第２セッション鍵を生成し、前記第１セッション鍵だけが前記ディジタル・ビデオ番組の非暗号化に有用になるように、第ｉセッション番号を非暗号化するためにそれぞれの第ｉ局所装置鍵を使用するためのコンピュータ可読コード手段を含む、上記（１５）のモジュール。

（１７）さらに、更新データを受信するためのコンピュータ可読コード手段を含み、前記モジュールが、１つまたは複数の新しい局所装置鍵を生成するために前記更新データを操作するために１つまたは複数の前記局所装置鍵を使用する、上記（１６）のモジュール。

（１８）さらに、放送メッセージに応答して、前記セッション鍵を他の装置のセッション鍵によって置換するためのコンピュータ可読コード手段を含む、上記（１７）のモジュール。

（１９）装置鍵の集合から選択された複数のコンピュータ使用可能装置鍵を複数のユーザ装置に供給するステップと、セッション鍵ブロックを作るために装置鍵の前記集合を用いて複数のセッション番号を暗号化する少なくとも１つのセッション鍵ブロック・ジェネレータを生成するステップと、前記ユーザ装置のうちの少なくとも１つが、暗号漏洩された装置鍵を定義する暗号漏洩された装置であることが判定された時に、前記セッション番号のうちの少なくとも１つがダミー番号になるように定義するステップと、暗号漏洩された装置鍵を用いて前記ダミー番号を暗号化するステップと、１つまたは複数の放送番組の非暗号化に使用するために前記セッション鍵ブロックを送信するステップと、前記ユーザ装置がセッション鍵の生成に前記ダミー番号を使用しない限り、前記番組を非暗号化するためにユーザ装置によって使用可能な前記セッション鍵を、前記セッション鍵ブロックおよび前記ユーザ装置のそれぞれの前記装置鍵に基づいて判定するために各ユーザ装置の前記装置鍵にアクセスするステップとを含む、前記１つまたは複数の放送番組の保護された送信のためのコンピュータ実施される方法。

（２０）装置鍵の前記集合が、鍵次元および集合次元を含む少なくとも２次元の行列によって表現可能であり、前記鍵次元が、鍵インデックス変数「ｉ」によってそれぞれが表される「Ｎ」個の鍵位置を表し、前記集合次元が、集合インデックス変数「ｊ」によってそれぞれが表される「Ｍ」個の集合を表し、各装置鍵を$S_{j,i}$によって表すことができるようになっている、上記（１９）の方法。

（２１）あるユーザ装置の２つの装置鍵のどれもが、互いに同一の鍵インデックス変数「ｉ」を有しない、上記（２０）の方法。

（２２）各セッション番号をx_iによって表すことができるように、鍵インデックス番号「ｉ」ごとにそれぞれのセッション番号を供給するステップと、前記セッション鍵ブロックを作るために、第ｉ鍵次元の装置鍵だけを用いて各セッション番号x_iを暗号化するステップとを含む、上記（２１）の方法。

（２３）前記暗号漏洩された装置鍵を有しないすべてのユーザ装置が、少なくとも第１セッション鍵を生成し、前記暗号漏洩された装置鍵を有するすべてのユーザ装置が、少なくとも第２セッション鍵を生成し、前記第１セッション鍵だけが、前記番組の非暗号化に有用になるように、各ユーザ装置が、第ｉセッション番号を非暗号化するためにそれぞれの第ｉ装置鍵$S_{j,i}$を使用する、上記（２２）の方法。

（２４）前記第１セッション鍵を生成するユーザ装置が、少なくとも第１プールを定義し、前記第２セッション鍵を生成するユーザ装置が、少なくとも第２プールを定義し、前記方法がさらに、前記第１プール内のすべてのユーザ装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に、前記第１プール内の前記ユーザ装置に、新しい装置鍵を生成するために前記ユーザ装置が操作する更新データを送信するステップを含む、上記（２３）の方法。

（２５）前記第２セッション鍵を生成するユーザ装置が、少なくとも第２プールを定義し、前記方法がさらに、前記第２プール内のすべてのユーザ装置が、暗号漏洩された装置であるかどうかを判定し、そうでない場合に、前記第２プール内のユーザ装置に新しいセッション鍵を生成させるステップを含む、上記（２３）の方法。

（２６）暗号漏洩されていない装置の第１集合が、第１プールを定義し、暗号漏洩されていない装置の第２集合が、第３プールを定義し、前記第１プールおよび前記第３プールのそれぞれが、暗号漏洩された装置を含まず、前記方法がさらに、前記第１プール内の装置に、前記第３プール内の前記装置の前記セッション鍵を用いてそれぞれのセッション鍵を置換させるステップを含む、上記（２３）の方法。

37

（２７）ディジタル処理装置によって読み取ることができるコンピュータ・プログラム記憶装置と、ディジタル番組の放送のためにこれを暗号化するための方法ステップを実行するために前記ディジタル処理装置によって実行可能な命令を含む、前記プログラム記憶装置上のプログラム手段とを含み、前記方法ステップが、ｉが１とＮを含む１からＮまでの整数であり、ｊが１とＭを含む１からＭまでの整数であり、「ｉ」が装置鍵$S_{j,i}$の行列の鍵次元での位置を示す鍵インデックス変数であり、「ｊ」が前記行列の集合次元での位置を示す集合インデックス変数であり、「Ｎ」が鍵のＭ個の集合のそれぞれの装置鍵の数であるものとして、前記装置鍵$S_{j,i}$の行列にアクセスするステップと、鍵インデックス変数「ｉ」ごとに各ディジタル・ビデオ装置に１つの装置鍵だけが割り当てられる形で、複数の前記ディジタル・ビデオ装置に、前記装置鍵の行列から複数の装置鍵を割り当てるステップと、ｉが１とＮを含む１からＮまでの整数であるものとして、それぞれが鍵インデックス変数「ｉ」に対応する複数のセッション番号x_iを生成するステップと、ｊが１とＭを含む１からＭまでの整数であるものとして、セッション鍵ブロックを生成するために、すべての装置鍵$S_{j,i}$を用いて各セッション番号x_iを暗号化するステップとを含む、コンピュータ・プログラム装置。

（２８）前記方法ステップがさらに、前記ディジタル・ビデオ装置のうちの１つまたは複数が暗号漏洩された装置であるかどうかを判定するステップと、前記暗号漏洩された装置の少なくとも１つの暗号漏洩された装置鍵によって暗号化されるダミー番号として、前記セッション番号のうちの少なくとも１つを作るステップとを含む、上記（２７）のコンピュータ・プログラム装置。

（２９）第１ディジタル・ビデオ装置が、第１セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第１ディジタル・ビデオ装置が、少なくとも第１プールを定義し、第２ディジタル・ビデオ装置が、第２セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第２ディジタル・ビデオ装置が、少なくとも第２プールを定義し、前記方法ステップがさらに、前記第１プール内のすべてのディジタル・ビデオ装置が暗号漏洩された装置でないかどうかを判定し、そうである場合に、新しい装置鍵を生成するために前記第１プール内の前記ディジタル・ビデオ装置が操作する更新データを前記第１プール内の前記ディジタル・ビデオ装置に送信するステップを含む、上記（２８）のコンピュータ・プログラム装置。

（３０）第２ディジタル・ビデオ装置が、第２セッション鍵を生成するために前記セッション鍵ブロックのうちの少なくとも一部を非暗号化し、前記第２ディジタル・ビデオ装置が、少なくとも第２プールを定義し、前記方

38

法ステップがさらに、前記第２プール内のすべてのディジタル・ビデオ装置が暗号漏洩された装置であるかどうかを判定し、そうでない場合は、前記第２プール内のディジタル・ビデオ装置に新しいセッション鍵を生成させるステップを含む、上記（２８）のコンピュータ・プログラム装置。

（３１）暗号漏洩されない装置の第１集合が、第１プールを定義し、暗号漏洩されない装置の第２集合が、第３プールを定義し、前記第１プールおよび前記第３プールのそれぞれが、暗号漏洩された装置を含まず、前記方法ステップがさらに、前記第１プール内の装置に、前記第３プール内の前記装置のセッション鍵を用いてそのセッション鍵を置換させるステップを含む、上記（２８）のコンピュータ・プログラム装置。

（３２）前記ディジタル・ビデオ装置と組み合わされた、上記（２７）のコンピュータ・プログラム装置。

（３３）ディジタル処理装置によって読み取ることができるコンピュータ・プログラム記憶装置と、ディジタル・ビデオ装置に少なくとも１つのディジタル番組を受信させ、提示させるための方法ステップを実行するために前記ディジタル処理装置によって実行可能な命令を含む、前記コンピュータ・プログラム記憶装置上のプログラム手段とを含み、前記方法ステップが、ｉが１とＮを含む１からＮまでの整数であり、ｊが１とＭを含む１からＭまでの整数であり、「Ｎ」が鍵のＭ個の集合のそれぞれの装置鍵の数であるものとして、各セッション番号x_iが第ｊ装置鍵$S_{j,i}$によって暗号化される暗号化されたセッション番号x_iを含む、少なくとも次元「ｉ」および「ｊ」を有する行列によって表すことのできるセッション鍵ブロックを受信するステップと、前記ディジタル・ビデオ装置に変数「ｉ」ごとに１つだけ割り当てられる複数の局所装置鍵にアクセスするステップと、前記局所装置鍵を使用して前記セッション鍵ブロックからのセッション鍵を非暗号化するステップとを含む、コンピュータ・プログラム装置。

（３４）前記方法ステップがさらに、前記ディジタル・ビデオ装置が暗号漏洩された装置鍵を有しない場合には、前記ディジタル・ビデオ装置が第１セッション鍵を生成し、前記ディジタル・ビデオ装置が１つまたは複数の暗号漏洩された装置鍵を有する場合には、前記ディジタル・ビデオ装置が第２セッション鍵を生成し、前記第１セッション鍵だけが前記ディジタル番組の非暗号化に有用になるように、第ｉセッション番号を非暗号化するためにそれぞれの第ｉ局所装置鍵を使用するステップを含む、上記（３３）のコンピュータ・プログラム装置。

（３５）前記方法ステップがさらに、更新データを受信するステップと、１つまたは複数の新しい局所装置鍵を生成するために、前記更新データを操作するのに１つまたは複数の前記局所装置鍵を使用するステップとを含む、上記（３４）のコンピュータ・プログラム装置。

39

（３６）前記方法ステップがさらに、放送メッセージに応答して、前記セッション鍵を他の装置のセッション鍵によって置換するステップを含む、上記（３５）のコンピュータ・プログラム装置。

【図面の簡単な説明】

【図１】本発明の放送暗号化システムのブロック図である。

【図２】コンピュータ・プログラム製品の概略図である。

【図３】装置鍵行列を示す図である。

【図４】放送番組の後続の非暗号化に使用するためにセッション鍵を暗号化し、ユーザ装置に送信し、非暗号化するための論理の流れ図である。

【図５】セッション鍵ブロックを示す図である。

【図６】セッション鍵計算メッセージを示す図である。

【図７】許可されない装置によって保持されていることが既知の少なくとも１つの装置鍵を使用する所定のダミー・セッション番号の暗号化のための論理の流れ図である。

【図８】図７の論理によって生成されるセッション鍵ブロックを示す図である。

【図９】装置のさまざまなプールを処理するために実行

40

される論理の流れ図である。

【図１０】条件付きセッション鍵計算メッセージを示す図である。

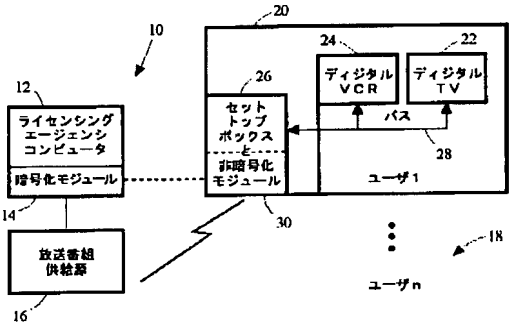
【図１１】セッション鍵変更メッセージを示す図である。

【図１２】装置鍵更新メッセージを示す図である。

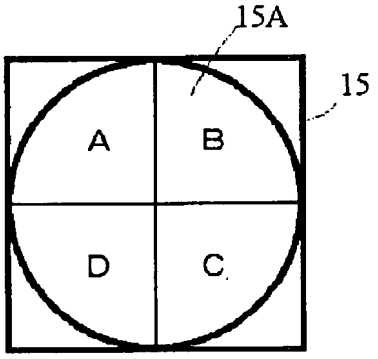
【符号の説明】

１０　システム
１２　ディジタル処理装置（コンピュータ）
１４　暗号化モジュール
１５　コンピュータ・ディスケット
１５Ａ　コンピュータ使用可能媒体
１６　放送番組供給源
１８　ビデオ装置
２０　ビデオ装置
２２　ディジタル・テレビジョン
２４　ディジタル・ビデオ・カセット・レコーダ（ＶＣＲ）
２６　セット・トップ・ボックス
２８　バス
３０　非暗号化モジュール

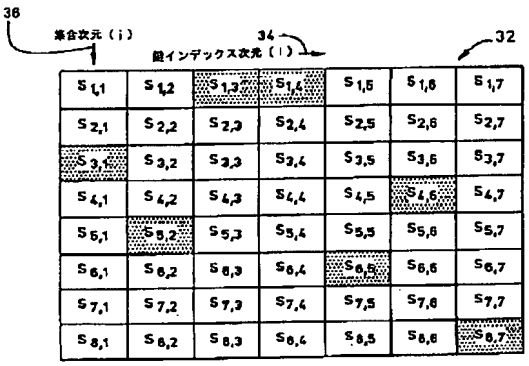
【図１】



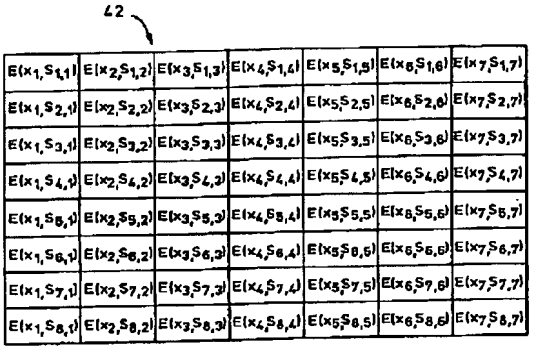
【図２】



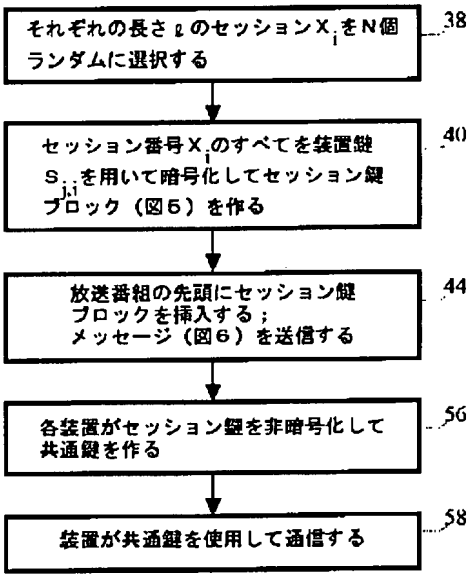
【図３】



【図５】

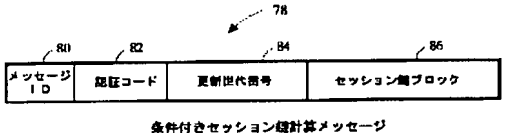


【図４】



【図６】

【図１０】



条件付きセッション鍵計算メッセージ

【図７】

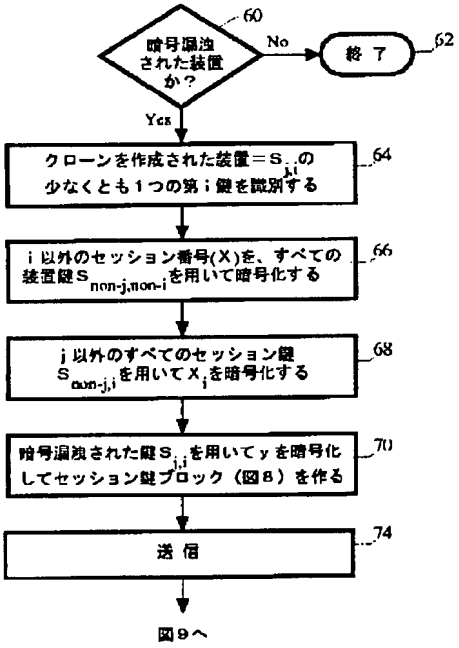
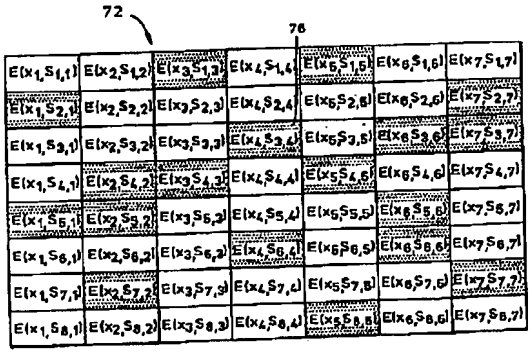
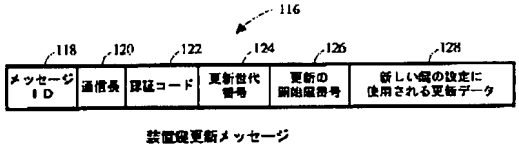


図９へ

【図８】

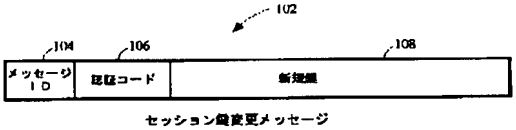


【図１２】



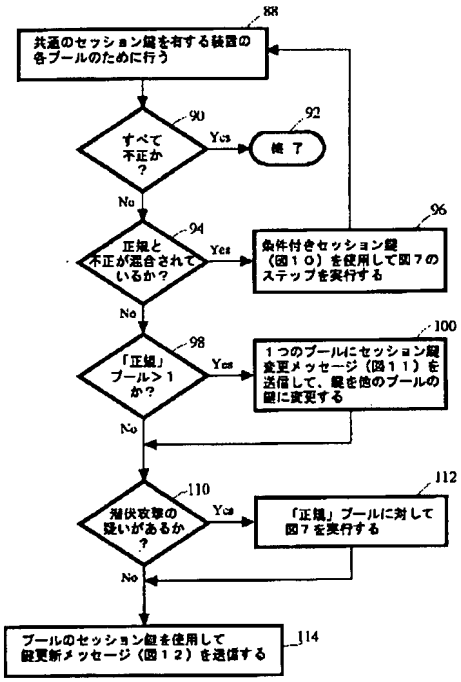
装置鍵更新メッセージ

【図１１】



セッション鍵変更メッセージ

【図９】



フロントページの続き

(72)発明者　ケヴィン・スノウ・マカーレイ
アメリカ合衆国95120　カリフォルニア州
サンノゼ　タナヒル・ドライブ　6721